Сканирование

5. Сканирование системы с помощью OpenVAS (GreenBone)

Примечание

Описаны все возможные пункты меню. Доступность конкретных функций зависит от модели решения в составе **НАЙС.ОС Greenbone COMMUNITY EDITION**.

5.1 Быстрый старт: мастер задачи

Мастер задачи позволяет запустить базовое сканирование с минимальным числом параметров.

5.1.1 Использование мастера задачи

1. Откройте *Scans* > *Tasks*.
2. Нажмите *New* и выберите *Task Wizard*.
3. Введите IP-адрес или имя хоста цели (см. рис. 5.1).

Рис. 5.1 — Настройка мастера задачи

Примечание: при использовании DNS-имени система должна уметь его разрешить.

4. Нажмите *Start Scan*.

Мастер автоматически:

- создаёт цель сканирования;
- создаёт задачу сканирования;

- немедленно запускает задачу;
- показывает страницу *Tasks*.

Прогресс отображается в списке задач (см. рис. 5.2). Подробности по статусам — см. разд. 5.8.

Рис. 5.2 — Страница задач с прогрессом сканирования

Совет

Отчёт доступен сразу после старта: нажмите индикатор в колонке *Status*. Чтение, управление и экспорт отчётов — см. гл. 6.

Полная версия отчёта появляется при статусе *Done*; промежуточные результаты доступны в ходе выполнения (см. разд. 6.2.1).

Сканирование может занять время; страница автоматически обновляется по мере появления данных.

5.1.2 Расширенный мастер задачи

Расширенный мастер предоставляет дополнительные параметры.

1. Откройте *Scans > Tasks*.
2. Нажмите *New* и выберите *Advanced Task Wizard*.
3. Заполните форму (см. рис. 5.3). Поля соответствуют настройкам из разд. 5.2.1 и 5.2.2.

Совет: если указать e-mail в поле *Email report to*, будет автоматически создано уведомление по завершении задачи (см. разд. 5.12).

Рис. 5.3 — Расширенный мастер задачи

4. Нажмите *Create*.

Задача будет немедленно запущена и показана на странице *Tasks*. Статусы — см. разд. 5.8. Работа с отчётами — см. гл. 6 (промежуточные результаты — см. разд. 6.2.1).

5.1.3 Мастер изменения существующей задачи

1. Откройте *Scans > Tasks*.
2. Нажмите *New* и выберите *Modify Task Wizard*.
3. Выберите изменяемую задачу в списке *Task* (см. рис. 5.4).

Рис. 5.4 — Изменение задачи через мастер

4. Создайте расписание, отметив *Create Schedule* (см. разд. 5.10), задайте дату и время первого запуска.
5. Укажите e-mail для рассылки отчёта в поле *Email report to*.
6. Нажмите *Modify Task*.

5.2 Ручная настройка простого сканирования

Есть два подхода к сканированию:

- **простое сканирование** (без учётных данных);
- **аутентифицированное** с локальными проверками безопасности.

Для простого сканирования выполните:

1. создайте цель (см. разд. 5.2.1);
2. создайте задачу (см. разд. 5.2.2);
3. запустите задачу (см. разд. 5.2.3).

5.2.1 Создание цели (Target)

1. *Configuration > Targets* *New*.
2. Заполните параметры (см. рис. 5.5) и нажмите *Save*.

Рис. 5.5 — Новая цель сканирования

Поля цели

- **Name** — произвольное осмысленное имя (например, *Mailserver*, *ClientNetwork*, *DMZ*).
- **Comment** — необязательно; контекст/описание.
- **Hosts** — перечисление объектов (через запятую) или импорт списка.
  Нужен IP-адрес или имя хоста, причём система должна иметь сетевую связность; для имён также требуется корректный DNS.

  Ограничение по количеству IP: для большинства моделей — до 4096; для OPENVAS SCAN 6500 — до 16 777 216.

  Поддерживаемые формы ввода IPv4:

  ```
  192.168.15.5
  mail.example.com
  192.168.15.5-192.168.15.27
  192.168.55.5-27
  192.168.15.0/24
  ```

  Из-за лимитов по количеству адресов максимальная маска по умолчанию — /20 для IPv4 (если нет других хостов в конфигурации). Классические network/broadcast адреса подсети в CIDR-диапазоне (например, 192.168.15.0 и 192.168.15.255) не считаются «используемыми» и не сканируются; добавьте их явно при необходимости.

  Поддерживаемые формы ввода IPv6:

  ```
  fe80::222:64ff:fe76:4cea
  ::12:fe5:fb50-::12:fe6:100
  ::13:fe5:fb50-fb80
  fe80::222:64ff:fe76:4cea/120
  ```

  Максимальная маска по умолчанию — /116 для IPv6 (с учётом лимита адресов). Более крупные маски допустимы на моделях с повышенным лимитом.

  Форматы можно смешивать; при импорте используется та же синтаксическая форма, разделители — запятые или переводы строк. Для больших наборов удобнее импорт из файла (ASCII). Также возможно добавление из базы активов (см. оговорку ниже).

  Импорт из базы активов доступен при создании цели со страницы *Hosts* (см.

разд. 8.1.3).
```

- **Exclude Hosts** — список исключений (форматы те же, допускаются также FQDN). Исключение по FQDN не «запрещает» IP для сканера (сканер IP-ориентирован), а исключает vhost-имя в рамках соответствующего IP.
- **Allow simultaneous scanning via multiple IPs** — для нестойких устройств (например, IoT) отключите одновременное сканирование по нескольким адресам одной цели, выбрав *No*.
- **Port list** — список портов для сканирования (см. разд. 5.7). Можно создать список «на лету» кнопкой рядом со списком.
- **Alive Test** — метод обнаружения доступности хоста:
  - *Use Scan Config Default* — по умолчанию ICMP Ping;
  - *Consider Hosts as Alive* — считать живыми (без проверки);
  - *Custom* — комбинации ICMP Ping, TCP-ACK Service Ping, TCP-SYN Service Ping, ARP Ping.

  Методы работают для IPv4/IPv6 (ICMPv6 для IPv6). При выборе ARP для IPv6 Boreas выполнит Neighbor Discovery. В некоторых средах возможны ложные ответы (RST от межсетевых экранов), а Proxy-ARP может давать «живые» ответы за хост — подбирайте метод под инфраструктуру (см. разд. 5.13).
- **SSH Credentials** — учётные данные для аутентифицированных проверок Linux/Unix (см. разд. 5.3 и 5.3.2).
- **Elevate Privileges** — экспериментальная поддержка повышения привилегий (например, до root). Требует выбранных SSH-учётных данных; затем появляется выбор учётных для повышения. Базовые и повышенные SSH-учётные данные не должны совпадать. Подробности — см. разд. 5.3.5.1.
- **SMB Credentials — Kerberos или NTLM** — для Windows-хостов (аутентифицированные проверки).
- **ESXi Credentials** — для VMware ESXi (аутентифицированные проверки).
- **SNMP Credentials** — для систем с поддержкой SNMP (аутентифицированные проверки).

  Любые учётные данные можно создать «на лету» кнопкой рядом со списком.
- **Reverse Lookup Only** — сканировать только IP, имеющие обратную DNS-запись.
- **Reverse Lookup Unify** — если несколько IP резолвятся в одно имя, сканировать его один раз.

  Для унификации предварительно проверяются все адреса, что на больших целях/медленном rDNS может надолго «застывать» на 1 % прогресса. Не рекомендуется для крупных сетей и сред с медленным rDNS.

```

5.2.2 Создание задачи (Task)

Задачи управляют запуском и расписанием сканов (см. разд. 5.10). Чтобы создать задачу:

1. *Scans > Tasks* *New Task*.
2. Заполните форму (см. рис. 5.6) и нажмите *Save*. Задача появится на странице *Tasks*.

Рис. 5.6 — Новая задача

Поля задачи

- **Name**, **Comment** — имя и описание.
- **Scan Targets** — выберите ранее созданную цель (см. разд. 5.2.1) или создайте её «на лету».
- **Alerts** — выберите оповещение (см. разд. 5.12) или создайте «на лету». Поддерживаются e-mail, Syslog, HTTP и коннекторы.
- **Schedule** — выберите расписание (см. разд. 5.10) или создайте «на лету» (например, «каждый понедельник 06:00»).
  Один и тот же расписанный запуск у большого числа задач может перегрузить систему вплоть до сбоя.
- **Add results to Assets** — автоматически добавлять обнаруженные системы в базу активов (см. гл. 8). Опцию можно менять позже.
- **Apply Overrides** — применять оверрайды при добавлении результатов в базу (см. разд. 6.8).
- **Min QoD** — минимальное качество детектирования для включения результатов в базу активов (см. разд. 6.2.6).
- **Alterable Task** — разрешить менять цели/сканер/конфигурацию скана даже после появления отчётов (нарушает консистентность отчётов между запусками).
- **Auto Delete Reports** — лимит числа отчётов; при превышении старые удаляются. По умолчанию — не удалять автоматически.
- **Scanner** — по умолчанию доступны встроенные *OpenVAS* и *CVE* (см. разд. 5.11). Внешние сенсоры — после настройки (см. гл. 11).
  Далее перечисленные параметры применимы только к *OpenVAS*; сканер *CVE* их не поддерживает.
- **Scan Config** — конфигурация набора VT и параметров сканера (см. разд. 5.9). В

задаче может быть только одна конфигурация.

- **Order for target hosts** — порядок обработки хостов: *Sequential*, *Random*, *Reverse*. Для улучшения оценки прогресса рекомендуется *Random* (см. разд. 12.2.3).
  Проверка доступности (alive test) всегда выполняется в случайном порядке.
- **Maximum concurrently executed NVTs per host / Maximum concurrently scanned hosts** — «скорость» сканирования. Значения по умолчанию подобраны безопасно. Увеличение параллелизма может негативно повлиять на целевые системы, сеть и саму платформу. Параметры соответствуют `maxchecks` и `maxhosts`.
- **Tag** — привязать тег к задаче (см. разд. 3.4).

5.2.3 Запуск задачи

1. В строке созданной задачи нажмите *Start*.

Примечание: у задач с расписанием отображается индикатор *Scheduled* — запуск произойдёт по времени, заданному в расписании (см. разд. 5.10).

Задача попадает в очередь ожидания, после чего сканер приступает к выполнению.

Примечание: в ряде случаев задача может «застрять» в очереди. Диагностика описана в разделе эксплуатации (см. подсистему мониторинга и логи сканера).

Статусы выполнения описаны в разд. 5.8. Отчёт доступен сразу после старта — нажмите индикатор в колонке *Status*. Чтение, управление и выгрузка отчётов — см. гл. 6. Полный отчёт доступен при статусе *Done*, при этом промежуточные результаты можно просматривать на всём протяжении выполнения (см. разд. 6.2.1).

Сканирование занимает время; страница автоматически обновляется при появлении новых данных.

5.3 Аутентифицированное сканирование (Local Security Checks)

Аутентифицированное сканирование дополняет внешний сетевой анализ проверками «изнутри» через валидный вход на целевую систему. Это повышает полноту инвентаризации патчей/ПО и точность детектов. Для выполнения LSC требуются заранее созданные учётные данные — они применяются к соответствующим службам на цели. Объём результатов зависит от прав учётной

записи.

VT из семейств локальных проверок запускаются только при успешном входе. Эти проверки минимально инвазивны: уровень риска определяется без изменений конфигурации цели. Факт входа фиксируется в журналах целевой системы.

Поддерживаемые направления доступа и типовые задачи:

- **SMB** (Windows) — уровень патчей, установленное ПО (Adobe Reader, Java и др.).
- **SSH** (Unix/Linux) — уровень патчей, инвентаризация пакетов.
- **ESXi** — локальные проверки VMware ESXi.
- **SNMP** — сетевое оборудование (маршрутизаторы, коммутаторы и пр.).

Метод	Порт(ы) по умолчанию	Поддерживаемые типы учётных данных
SMB	`445/TCP, 139/TCP`	Username + Password
SSH	`22/TCP` (можно переопределить в цели)	Username + Password; Username + SSH Key
ESXi	Согласно документации Broadcom/VMware	Username + Password
SNMP	`161/UDP`	SNMP (v1/v2c Community; v3 user+auth+privacy)

5.3.1 Плюсы и ограничения аутентифицированных сканов

Результаты зависят от уровня прав. На Linux достаточно непривилегированной учётной записи для доступа к большинству важных сведений; в Windows непривилегированные учётные записи сильно ограничены (реестр и `\Windows` недоступны), поэтому администраторские права дают существенно больше данных.

LSC — самый «щадящий» способ уточнения уязвимостей. Дистанционные проверки также минимально инвазивны, но иногда могут влиять на сервисы.

- **Аутентифицированное сканирование** — аналог Whitebox: известен контекст, доступ изнутри (реестр, версии ПО, патч-уровни).
- **Удалённое сканирование** — аналог Blackbox: техники злоумышленника

«снаружи», аппарат собирает сведения сам, иногда провоцируя реакции сервисов для извлечения версии/баннера.

В конфигурации *Full and fast* все удалённые проверки считаются безопасными благодаря `safe_checks=yes` — высоко-инвазивные/DoS-проверки исключены.

Пример инвазивного, но безопасного VT

Проверка Heartbleed исполняется даже при включённых *safe_checks*, т.к. не нарушает работоспособность цели. Она всё же инвазивна, поскольку проверяет утечку памяти: если уязвимость есть, часть памяти возвращается в ответе. Аппарат не анализирует содержимое и немедленно его отбрасывает.

5.3.2 Работа с учётными данными

Учётные данные нужны для входа на цель и выполнения локальных проверок (проверка наличия вендорных патчей и др.).

5.3.2.1 Создание учётных данных

1. *Configuration > Credentials* *New*.
2. Заполните форму (см. рис. 5.7) и нажмите *Save*.

Рис. 5.7 — Новые учётные данные

Важно: привяжите учётные данные хотя бы к одной цели — иначе движок не сможет их применить.

Поля и типы

- **Name** — произвольное имя; **Comment** — опционально.
- **Type** — варианты: *Username + Password*, *Username + SSH Key*, *SNMP*, *S/MIME Certificate*, *PGP Encryption Key*, *Password only*, *SMB (Kerberos)*.
- **Allow insecure use** — разрешить применение в незашифрованных/потенциально небезопасных схемах аутентификации.

Username + Password

- **Auto-generate** — автогенерация пароля (при включении поле *Password* недоступно).
- **Username** — допустимы: латинские буквы/цифры, -, _, \, ., @. Немецкие умляуты заменяются: ß□ss, ä□a, ö□o, ü□u.
- **Password** — пароль для входа.

Username + SSH Key

- **Auto-generate** — автогенерация пароля (не для ключа).
- **Username** — те же правила допустимых символов.
- **Passphrase** — парольная фраза приватного ключа.
- **Private Key** — загрузка приватного ключа: поддержка Ed25519, ECDSA, RSA, DSA; форматы PEM/OpenSSH (для DSA — только OpenSSH).
  Конвертация DSA PEM□OpenSSH:

  ```
  ssh-keygen -p -f <private_key>
  ```

  Команда перезаписывает файл — сохраните копию, если нужен исходный PEM.

SNMP

Для SNMPv3 требуются имя пользователя, пароль аутентификации и пароль шифрования; для v1/v2c — только community.

Стек SNMP пробует все версии: можно увидеть одновременно «Login Successful» и «Login Failed» для разных версий.

- **SNMP Community** (v1/v2c), **Username** (v3; те же правила символов), **Password** (v3), **Privacy Password** (v3), **Auth Algorithm** (MD5/SHA1), **Privacy Algorithm** (AES/DES/none).

S/MIME Certificate

- Загрузите X.509 сертификат в PEM, действительный (не истёкший) и содержащий всю цепочку (root+intermediate). Если исходный бандл включал приватный ключ, загрузите только нешифрованный сертификат.

PGP Encryption Key

- Загрузите публичный ключ PGP.

Password only

- Пароль для целевой системы (используется сценариями, где логин формируется иначе).

SMB (Kerberos)

Для Kerberos требуется DNS с корректным reverse lookup целевого хоста (то же — для сенсора, если скан идёт через сенсор). При неудаче Kerberos выполняется откат на NTLM.

- **Username** — правила символов как выше; **Password**.
- **Realm** — в верхнем регистре, например `EXAMPLE.COM`.
- **KDC** — один или несколько KDC по имени или IP (добавляйте по Enter). Открыты порты `88/UDP` и `88/TCP`.

5.3.2.2 Управление учётными данными

Configuration > Credentials — список всех записей с полями **Name**, **Type**, **Allow insecure use**, **Login** (если применимо).

Действия: переместить в корзину (если не используются), редактировать, клонировать, экспортировать в XML. Под списком доступны массовые операции.

Дополнительные действия зависят от типа:

- Скачивание EXE (Windows) — для *Username + Password*.
- Скачивание RPM (RHEL-подобные) и DEB (Debian-подобные), а также публичного ключа — для *Username + SSH Key*.

Пакеты упрощают подготовку целей к аутентифицированным проверкам: создают пользователя, минимально необходимые привилегии и чисто удаляются. При включённой авто-генерации паролей использование пакетов обязательно; иначе — по желанию.

Страница деталей учётных данных содержит вкладки *Information*, *User Tags* (см. разд. 3.4), *Permissions* (см. разд. 4.4), и набор контекстных действий (открыть справку, перейти к списку, создать/клонировать/редактировать/удалить, экспортировать), а также упомянутые артефакты для скачивания в зависимости от типа.

5.3.3 Требования к целевым системам Microsoft Windows

5.3.3.1 Общие указания по конфигурации

Для корректной работы аутентифицированных проверок на Windows-целях необходимо обеспечить несколько системных условий. Документ ниже содержит рекомендуемые настройки и предостережения — применяйте их с учётом корпоративной политики и правил безопасности.

- **Служба «Remote Registry»** (Удалённый реестр) должна быть доступна во время сканирования. Обычно её настраивают на автоматический запуск; допустим и режим ручного запуска — в этом случае служба запускается на время скана и затем отключается. ```
- Необходимо включить **File and Printer Sharing**. Для Windows XP отключите опцию *Use Simple File Sharing*.
- Для автономных систем (не в домене) требуется выставить реестровое значение:

  ```
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
  ```

  ```
  DWORD: LocalAccountTokenFilterPolicy = 1
  ```

  ```
- На контроллерах домена для наилучших результатов используйте учетную запись, входящую в группу *Domain Administrators*. Локальные администраторские учётные записи не всегда дают полный набор обнаруживаемых результатов из-за модели прав.
- Если всё же используется локальный администратор (что не рекомендуется), необходимо также выставить:

  ```
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
  ```

  ```
  DWORD: LocalAccountTokenFilterPolicy = 1
  ```

  ```
- Сгенерированный установочный пакет для учётных данных (installer), предоставляемый платформой, автоматически выставляет Remote Registry в

автозапуск и может добавлять пользователя в группу BUILTIN\Administrators при установке на контроллере домена.
- На целевой машине создайте исключение для IP сканера в брандмауэре Windows; установщик может предложить ввести IP аплайенса и автоматически настроить правило фаервола. На Windows XP дополнительно включается служба File and Printer Sharing.
- **Выполнение PowerShell** — некоторые политики и VT выполняют PowerShell-команды для точности результатов. Аккаунт, используемый для сканирования, может потребовать права на выполнение PowerShell. При необходимости настройте исключения и контроль исполнения.
- Для аудитов соответствия (compliance) рекомендуется снижать параллелизм: установите *Maximum concurrently executed NVTs per host* и *Maximum concurrently scanned hosts* в `1`, чтобы повысить точность (см. раздел с рекомендациями по производительности).
- Для корректной работы WMI (например, поиск файлов, policy scans) требуется:
  - разрешить WMI в настройках Windows Firewall (или третьестороннего брандмауэра);
  - пользователь/группа сканера должны иметь удалённый доступ к WMI;
  - убедиться, что в среде допустим запуск инструментов типа *Impacket*, которые используются платформой для удалённого выполнения команд — при наличии средств защиты их исполнение может трактоваться как вредоносное и блокироваться.
- Убедитесь, что ресурс `ADMIN$` доступен для чтения/записи (нужен для некоторых операций).
- Рекомендуемая минимальная версия PowerShell — **PS 5.1 (WMF 5.1)**. Команды могут работать и на старших/младших версиях, но гарантии нет.
- Для аутентификации через Kerberos используйте доменную учётную запись; желательно, чтобы эта учётная запись имела локальные права администратора на цели. Для сканирования контроллера домена требуются права Domain Administrator. ```

## 5.3.3.2 Настройка доменной учётной записи для аутентифицированных сканов

Для масштабируемых и безопасных проверок настоятельно рекомендуется использовать доменную учётную запись с политикой, предоставляющей локальные права администратора. Это упрощает администрирование, минимизирует ручные

правки реестра и даёт возможность обнаруживать доменно-специфичные результаты.

**Преимущества доменной учётной записи с GPO:**

- централизованное управление правами (GPO применяет/отзывает настройки);
- не нужно вручную править реестр на каждой машине;
- динамическая защита учётных данных — Kerberos снижает риск утечки пароля по сравнению с локальной учётной записью;
- возможность запрещать локальный вход и вход по RDP для уменьшения векторов атаки.

Процесс примерной настройки (на контроллере домена):

#### Создание группы безопасности

1. Откройте *Active Directory Users and Computers* на контроллере домена.
2. Action → *New* → *Group*.
3. Имя: **NiceOS Local Scan** (рекомендуемое имя).
4. Group Scope: *Global*, Group Type: *Security*.
5. Добавьте учётную запись сканера в созданную группу. Нажмите *OK*.

#### Создание Group Policy Object (GPO)

1. Откройте *Group Policy Management*.
2. Правый клик на *Group Policy Objects* → *New*.
3. Введите имя GPO: **NiceOS Local SecRights**. Нажмите *OK*.

Рис. 5.8 — Создание *GPO* для локальных сканов

#### Настройка политики — добавление в локальные администраторы

1. Выберите созданный GPO и нажмите *Edit*.
2. Перейдите: *Computer Configuration* → *Policies* → *Windows Settings* → *Security Settings*.
3. Откройте *Restricted Groups* → *Add Group* → *Browse...* → введите **NiceOS Local Scan** и *Check Names*.
4. В разделе *This group is member of* добавьте группу **Administrators** (на недвухязычных системах укажите локальное имя администраторов).

Рис. 5.9 — Подтверждение имён групп

#### Запрет локального и RDP-входа для группы сканирования

1. В GPO: *Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment*.
2. Откройте *Deny log on locally*, активируйте и добавьте **NiceOS Local Scan** → *Check Names* → сохранить.
3. Аналогично откройте *Deny log on through Remote Desktop Services* и добавьте ту же группу. Сохраните.

Рис. 5.10 — Настройка отказа в локальном входе

#### Ограничение прав на реестр (опционально)

**Внимание:** изменение прав на ветви реестра через GPO «tattoos» — эти изменения сохраняются на системе даже после удаления GPO. Тщательно протестируйте.

1. В GPO: *Computer Configuration → Policies → Windows Settings → Security Settings → Registry → Add Key*.
2. Добавьте ключ `USERS`, нажмите *Advanced → Add* и выберите группу **NiceOS Local Scan**.
3. Для этой группы снимите все Allow-флаги и поставьте Deny для действий: *Set Value, Create Subkey, Create Link, Delete, Change Permissions, Take Ownership*. Подтвердите предупреждение.
4. Отметьте *Configure this key then* и *Propagate inheritable permissions to all subkeys*, нажмите *OK*.
5. Повторите для ветвей `MACHINE` и `CLASSES_ROOT`.

Рис. 5.11 — Выбор ключа реестра для ограничения

**Связывание GPO с доменом**

1. В консоли Group Policy Management правым кликом по домену выберите *Link an Existing GPO...*.
2. Выберите **NiceOS Local SecRights** и нажмите *OK*.

Рис. 5.12 — Привязка *GPO* к домену

## 5.3.3.3 Ограничения

При снятии прав на запись в реестр и системный диск некоторые тесты не будут работать:

- **Leave information on scanned Windows hosts** (OID `1.3.6.1.4.1.25623.1.0.96171`) — тест пытается записать информацию о старте/окончании скана под `HKLM\Software\VulScanInfo`. При запрете записи тест невозможен.
- **Windows file Checksums** (OID `1.3.6.1.4.1.25623.1.0.96180`) — тест сохраняет утилиту ReHash в `C:\Windows\system32` или `C:\Windows\SysWOW64`. При запрете записи тест не выполнится; можно разместить инструмент вручную или скорректировать GPO.

Дополнительные сведения — в разделе с продвинутыми VT и политиками (см. разделы по конфигурации сканера и политикам).

## 5.3.3.4 Сканирование без прав Domain Administrator / Local Administrator

Теоретически возможно построить GPO, в котором учетная запись не имеет локальных прав администратора, но тогда требуется вручную давать детальные права на чтение отдельных веток реестра и каталогов. Это трудозатратно, часто несовместимо с наследованием прав (inheritance часто отключено) и приводит к «tattooing» (изменения сохраняются после удаления GPO).

С практической и административной точки зрения подобная схема редко оправдана.

## 5.3.4 Требования к целевым системам ESXi

Если ESXi управляется через VCSA (vCenter Server Appliance) и пользователи созданы на VCSA, они известны только VCSA, но не самим ESXi-хостам. Для корректного сканирования учётные записи необходимо создавать на каждом ESXi-хосте, который будет сканироваться.

По умолчанию локальные пользователи ESXi имеют ограниченные права «read-only». Для корректной работы требуется либо административная учётная запись, либо роль «Read-only with Global Settings».

#### Пример: создание роли с правом доступа к глобальным настройкам

1. Откройте веб-интерфейс ESXi и войдите.
2. Host  Manage  Security & users  Roles  Add role.
3. Введите имя роли и включите опцию *System*. Нажмите *Global*  отметьте *Settings*. Нажмите *Add*.
4. Host  Permissions  выберите аккаунт сканирования  Assign role  выберите созданную роль  Assign role  Close.

Рис. 5.13 — Управление ролями в *ESXi*

## 5.3.5 Требования к целевым системам Linux/Unix

Для аутентифицированных сканов Linux/Unix обычно достаточно обычной (non-privileged) учётной записи, доступной по SSH. Аутентификация реализуется паролем или приватным SSH-ключом, хранящимся на платформе.

#### Рекомендации для SSH-сервера

- Рекомендуемые значения в `sshd_config`:

  ```
  MaxSessions 10
  MaxAuthTries 6
  ```

  При меньших или нестандартных значениях возможны сбои при множественных попытках входа.

- Убедитесь, что `PubkeyAuthentication yes` и публичный ключ корректно установлен с правами 600/700.
- Поддерживаемые типы ключей: Ed25519, ECDSA, RSA, DSA (DSA — только OpenSSH-формат для приватного ключа).

Установочные пакеты учётных данных

Инсталляторы генерируемых пакетов для Linux:

- Debian-подобные — `.deb`;
- RHEL-подобные — `.rpm`;
- Другие дистрибутивы — предлагается загрузить публичный ключ для ручной установки.

Пакет создаёт пользователя без дополнительных полномочий и помещает публичный ключ в домашнюю директорию. За корректность прав и конфигурацию отвечает администратор целевой системы.

Права и команды, исполняемые при аутентифицированном скане

Для некоторых проверок могут потребоваться повышенные (root) права или членство в специальных группах (например, `wheel`). Чем выше привилегии аккаунта, тем более детальные данные будут доступны; в ряде случаев нужен root-доступ.

Примеры команд, которые могут быть выполнены с правами root в процессе LSC (список не является исчерпывающим):

```
bash
cat
date
dpkg
egrep
find
grep
host
id
ip
lastlog
locate
ls
md5sum
mlocate
netstat
perl
ps
```

```
rpm
sh
sha1sum
slocate
uname
uptime
whereis
which
```

Рекомендуется установить на цели пакет `locate` (или `mlocate`) и обеспечить регулярное обновление его базы (например, cron), чтобы ускорить операции поиска и снизить нагрузку, которую в противном случае создаёт `find`.

Команды и набор выполняемых операций могут меняться с выходом новых VT — учитывайте это при планировании прав доступа.

5.3.5.1 Требования и общая информация по функции Elevate Privileges

- Права «повышенного» пользователя должны быть настроены на целевой системе заранее. Платформа лишь выполняет `su - <username>` и не управляет моделью разрешений.
- При задании «elevated SSH credentials» обычные SSH-учётные данные используются только для входа; для самих проверок применяются повышенные.
- Для «повышенного» пользователя должны быть доступны утилиты `stty`, `unset` и `bind`.
- Пользователь с повышенными правами должен иметь возможность менять приглашение оболочки (допускается `export PS1=...`, добавляемый к командам).
- Если настроены elevated SSH-учётные данные, они будут использованы всегда, даже если в конфигурации сканирования нет соответствующих VT.
- Нельзя указывать одинаковые обычные и повышенные SSH-учётные данные.
- Поддерживается только оболочка **bash**.

Статус: функция экспериментальная. Надёжность зависит от целевой системы и её конфигурации. Использование повышенных SSH-учётных данных увеличивает нагрузку на платформу и число SSH-сессий (учтите правила на межсетевых экранах, IDS/IPS и в системах журналирования). Из-за этого сканы могут выполняться заметно дольше.

5.3.5.2 Рекомендации безопасности для SSH-основанных аутентифицированных сканов

- Не сканируйте широкие диапазоны сети с присвоенными SSH-учётными данными. Формируйте целевые списки известных хостов с явными IP-адресами.
- Используйте минимально необходимые привилегии: отдельная учётная запись сканирования вместо `root`.
- Проводите аутентифицированные проверки только доверенных систем, не запускайте такие проверки по общедоступным ресурсам.

5.3.6 Требования к системам с Cisco OS

Сетевые устройства (маршрутизаторы, коммутаторы) могут проверяться как удалённо (сетевые сервисы), так и аутентифицированно (SNMP/SSH). Ряд уязвимостей выявляется только при аутентифицированном доступе.

5.3.6.1 SNMP

Поддерживаются SNMPv1/v2c/v3 (порт `161/UDP`). В типовой порт-листе UDP отсутствует, поэтому SNMP-проверки в профиле «Full and fast» будут игнорироваться. Создайте отдельный порт-лист для сетевого оборудования, включив минимум:

```
22/TCP SSH
80/TCP 8080/TCP HTTP
443/TCP 8443/TCP HTTPS
2000/TCP SCCP
2443/TCP SCCPS
5060/TCP 5060/UDP SIP
5061/TCP 5061/UDP SIPS
67/UDP DHCP Server
69/UDP TFTP
123/UDP NTP
161/UDP SNMP
162/UDP SNMP Traps
500/UDP IKE
514/UDP Syslog
546/UDP DHCPv6
6161/UDP 6162/UDP Unified CM
```

Для минимально необходимого доступа используйте SNMP-view, ограничивающий видимость MIB.

Пример (community string)

```
# configure terminal
(config) # access-list 99 permit 192.168.222.74
(config) # snmp-server view gsm system included
(config) # snmp-server view gsm system.9 excluded
(config) # snmp-server community gsm-community view gsm RO 99
```

Пример (SNMPv3 с шифрованием)

```
# configure terminal
(config) # access-list 99 permit 192.168.222.74
(config) # snmp-server view gsm system included
(config) # snmp-server view gsm system.9 excluded
(config #) snmp-server group gsmgroup v3 priv read gsm access 99
(config #) snmp-server user gsm-user gsm-group v3 auth md5 gsm-password priv aes 128 gsm-encrypt
```

Затем создайте соответствующие SNMP-учётные данные в интерфейсе: *Configuration → Credentials* (см. разд. 5.3.2).

5.3.6.2 SSH

Аутентифицированный доступ возможен и по SSH. Рекомендуется отдельный непривилегированный пользователь, которому разрешено выполнять только необходимые команды. Для идентификации прошивки достаточно `show version`.

Перед применением убедитесь в последствиях включения RBAC/views: при ошибке можно блокировать авторизацию по SSH/консоли.

Включение AAA и views

```
> enable
# configure terminal
(config)# aaa new-model
(config)# exit
> enable view
# configure terminal
```

Создание ограниченного view (только `show version`)

```
(config)# parser view gsm-view
(config-view)# secret 0 view-pw
(config-view)# commands exec include show version
```

```
(config-view)# exit
(config)# username gsm-user view gsm-view password 0 gsm-pw
(config)# aaa authorization console
(config)# aaa authorization exec default local
```

Включение SSH

```
(config)# hostname switch
(config)# ip domain-name example.net
(config)# crypto key generate rsa general-keys modulus 2048
(config)# line vty 0 4
(config-line)# transport input ssh
(config-line)# end
```

Для полноценных сканов (например, «Full and fast») проверьте значение `ssh server rate-limit` — рекомендуется `240`.

Создайте SSH-учётные данные (*Configuration → Credentials*) и привяжите их к цели.

5.3.7 Требования к системам с Huawei VRP

Поддерживаются аутентифицированные проверки по SNMP или SSH. Команды ниже — ориентир; синтаксис может отличаться по версиям ПО и моделям оборудования. Пользуйтесь официальной документацией конкретного устройства.

5.3.7.1 SNMP

Как и в случае Cisco, включите UDP-порты в порт-лист (см. перечень в разд. 5.3.6.1). Для ограниченного доступа создайте MIB-view и примените ACL.

Пример (community v2c)

```
<HUAWEI>system-view
[~HUAWEI]acl 2000
[~HUAWEI-acl4-basic-2000]rule permit source 192.168.222.74 32
[*HUAWEI-acl4-basic-2000]commit
[~HUAWEI-acl4-basic-2000]quit
[~HUAWEI]snmp-agent sys-info version v3 v2c
[*HUAWEI]commit
[~HUAWEI]snmp-agent mib-view included gsm system
[*HUAWEI]snmp-agent mib-view excluded gsm system.9
[*HUAWEI]commit
[~HUAWEI]snmp-agent community read gsm-community mib-view gsm acl 2000
```

```
[*HUAWEI]commit
```

Пример (SNMPv3 с шифрованием)

```
<HUAWEI>system-view
[~HUAWEI]acl 2000
[~HUAWEI-acl4-basic-2000]rule permit source 192.168.222.74 32
[*HUAWEI-acl4-basic-2000]quit
[*HUAWEI]snmp-agent sys-info version v3
[*HUAWEI]snmp-agent mib-view included gsm system
[*HUAWEI]snmp-agent mib-view excluded gsm system.9
[*HUAWEI]commit
[~HUAWEI]snmp-agent group v3 gsmgroup privacy read-view gsm acl 2000
[*HUAWEI]commit
[~HUAWEI]snmp-agent usm-user v3 gsm-user authentication-mode md5
# введите пароль аутентификации (8–255)
[*HUAWEI]commit
[~HUAWEI]snmp-agent usm-user v3 gsm-user privacy-mode aes128
# введите пароль шифрования (8–255)
[*HUAWEI]commit
[*HUAWEI]snmp-agent usm-user v3 gsm-user group gsmgroup
[*HUAWEI]commit
```

Затем создайте соответствующие SNMP-учётные данные в интерфейсе: *Configuration → Credentials* (см. разд. 5.3.2).

5.3.7.2 SSH (Huawei VRP)

Аутентифицированные проверки Huawei VRP можно выполнять по SSH. Рекомендуется выделенный непривилегированный пользователь, которому разрешён ограниченный набор команд. Для идентификации версии прошивки достаточно следующих запросов:

```
display device
display version
display patch-information
```

Примечание по compliance-аудитам. В профилях соответствия могут дополнительно применяться команды:

```
display arp speed-limit
display arp-miss speed-limit source-ip
display current-configuration
display current-configuration configuration bgp
```

```
display current-configuration configuration pim
display current-configuration configuration user-interface
display current-configuration configuration vpn-instance
display current-configuration interface
display current-configuration | include multicast
display current-configuration | include ntp
display current-configuration | include snmp
display current-configuration | include ssh
display ftp-server
display isis peer
display mpls ldp session verbose
display mpls rsvp-te interface
display ospf peer brief
display ospfv3 peer
display snmp-agent sys-info version
display ssh server status
display telnet server
display telnet server status
display vrrp
```

Ниже пример настройки RBAC-профиля, ограничивающего пользователя только указанными командами. Перед внедрением оцените побочные эффекты: при ошибках можно ограничить входы по SSH/консоли.

Создание локального пользователя и разрешение SSH/STelnet

```
<HUAWEI> system-view
[~HUAWEI] aaa
[~HUAWEI-aaa] local-user gsm-user password cipher Hello-secret123
[*HUAWEI-aaa] local-user gsm-user level 0
[*HUAWEI-aaa] local-user gsm-user service-type ssh
[*HUAWEI-aaa] commit
[~HUAWEI-aaa] quit
[~HUAWEI] ssh user gsm-user authentication-type password
[*HUAWEI] ssh user gsm-user service-type stelnet
[*HUAWEI] commit
```

Ограничение набора команд для уровня 0

```
[~HUAWEI] command-privilege level 0 view global display device
[*HUAWEI] command-privilege level 0 view global display version
[*HUAWEI] command-privilege level 0 view global display patch-information
[*HUAWEI] commit
```

Включение SSH, VTY и STelnet

```
[~HUAWEI] rsa local-key-pair create
[*HUAWEI] commit

[~HUAWEI] user-interface vty 0 4
[*HUAWEI-ui-vty0-4] authentication-mode aaa
[*HUAWEI-ui-vty0-4] protocol inbound ssh
[*HUAWEI-ui-vty0-4] quit
[*HUAWEI] commit

[~HUAWEI] stelnet server enable
[*HUAWEI] ssh authentication-type default password
[*HUAWEI] commit
```

Ограничение доступа по IP (ACL)

Это ограничение заблокирует SSH-входы с других адресов. Используйте осторожно, чтобы не потерять удалённый доступ.

```
[~HUAWEI] acl 2000
[*HUAWEI-acl4-basic-2000] rule permit source 192.168.222.74 32
[*HUAWEI-acl4-basic-2000] quit
[*HUAWEI] acl 2000
[*HUAWEI] commit
```

На некоторых конфигурациях система попросит сменить пароль при первом входе — проверьте, выполнив ручной SSH-вход.

Затем в веб-интерфейсе НАЙС.ОС (OPENVAS SCAN) создайте SSH-учётные данные и привяжите их к цели: *Configuration Credentials* (см. разд. 5.3.2).

5.3.8 Требования к целевым системам EulerOS

Для EulerOS обычно достаточно обычной учётной записи с доступом по SSH. Аутентификация — паролем либо приватным ключом, хранящимся на аплаенсе.

- Генерируемый инсталлятор учётных данных — `.rpm`; он создаёт пользователя без дополнительных привилегий и размещает публичный ключ в домашнем каталоге.
- В `sshd` не должно быть запрета на ключевую аутентификацию (`PubkeyAuthentication`

`no` недопустим).
- Можно использовать существующие пары ключей (Ed25519/ECDSA/RSA/DSA); приватный ключ — в формате PEM или OpenSSH (для DSA — только OpenSSH).
- Для политик могут потребоваться *root* либо членство в группах (например, `wheel`), т.к. часть конфигураций доступна только привилегированным пользователям.

Команды, которые могут выполняться с правами root (перечень нефиксированный, зависит от дистрибутива и VT):

```
bash
cat
date
dpkg
egrep
find
grep
host
id
ip
lastlog
locate
ls
md5sum
mlocate
netstat
perl
ps
rpm
sh
sha1sum
slocate
uname
uptime
whereis
which
```

Рекомендуется установить `locate`/`mlocate` и настроить регулярное обновление базы (cron) — это ускоряет поиск и снижает нагрузку по сравнению с повсеместным `find`.

5.3.9 Требования к целевым системам GaussDB

Перед запуском убедитесь, что скан выполняется пользователем, имеющим права на

выполнение GaussDB (доступ к zsql/zengine и переменным окружения).

5.3.9.1 Пользователь root (не рекомендуется)

На аплаенсе: добавьте учётные данные (пароль или SSH-ключ).
На цели: root может запускать `zsql`/`zengine` (например, корректно задан `LD_LIBRARY_PATH`); в `sshd_config` разрешён root-доступ: `PermitRootLogin yes` либо `prohibit-password` для ключевой аутентификации.

5.3.9.2 Администратор БД (напр. gaussdba)

На аплаенсе: пароль/ключ для хоста(ов).
На цели: пользователь `gaussdba` — инсталляционный пользователь СУБД.

5.3.9.3 Обычный пользователь ОС

На аплаенсе: пароль/ключ для хоста(ов).
На цели: пользователь способен выполнить `zsql`/`zengine` (включая корректный `LD_LIBRARY_PATH`).

5.3.9.4 Обычный пользователь БД (напр. gauss)

На аплаенсе: учётные данные пользователя `gauss` и пароль, заданный в каждой используемой конфигурации сканирования.
На цели: открытый наружу порт сервера БД.

5.4 Настройка сканирования CVE

Для оперативной оценки рисков без повторного полного скана можно использовать CVE-сканер. Он сопоставляет обнаруженные ранее CPE целевых хостов с актуальными CVE из базы SecInfo и формирует прогноз уязвимостей.

Ограничения метода. CVE-сканер не подтверждает фактическое наличие уязвимости и не учитывает «бэкапорты» исправлений в дистрибутивах. Возможны ложноположительные результаты.

Предпосылки для корректной работы

- В NVD у CVE должен быть задан корректный CPE.
- Для формирования перечня продуктов должны быть актуальные данные в базе активов: ранее выполните полный скан (например, «Full and fast») с опцией *Add results to Assets = Yes*.
- Аутентифицированные полные сканы улучшают наполнение CPE и качество прогноза.
- Полные сканы рекомендуется выполнять регулярно; проверяйте вкладку *Applications* в отчёте полного скана, чтобы удостовериться в детектировании продуктов.

Порядок запуска CVE-сканирования

1. Выполните полный скан (см. разд. 5.2 и 5.3) с *Add results to Assets = Yes*.
2. Откройте *Scans → Tasks* и создайте задачу (*New Task*).
3. В поле *Scanner* выберите **CVE**, заполните остальные параметры и сохраните.
4. Запустите задачу. Прогресс см. в статус-баре; промежуточные результаты доступны по клику на индикаторе статуса.

По завершении откройте *Scans → Reports*, выберите отчёт по дате — в нём перечислены обнаруженные CVE по идентификатору (см. рис. 5.21).

Рис. 5.21 — Результаты *CVE*-сканирования

Клик по записи CVE откроет карточку с подробной информацией и доступными действиями (см. разделы по работе с отчётами).

Рис. 5.22 — Детали обнаруженного *CVE*

5.5 Импорт отчётов (Import Tasks)

В НАЙС.ОС Greenbone COMMUNITY EDITION (OPENVAS SCAN) импорт-задачи используются для загрузки и публикации отчётов, созданных на других инсталляциях/аплаенсах. Это удобно при миграции, консолидации или обмене

результатами аудитов.

5.5.1 Создание импорт-задачи

1. Откройте *Scans → Tasks*.
2. Нажмите *New* и выберите **New Import Task**.
3. Укажите имя задачи в поле *Name* (см. рис. 5.23).

Рис. 5.23 — Создание импорт-задачи

4. Нажмите **Save**.
5. В строке импорт-задачи нажмите **Import Reports**.
6. Выберите XML-файл отчёта (см. рис. 5.24).

Рис. 5.24 — Добавление отчёта в импорт-задачу

7. При необходимости включите добавление результатов в базу активов, выбрав **Yes** (см. гл. 7 «Управление активами»).
8. Нажмите **Import**.

5.5.2 Управление импорт-задачами

Список импорт-задач доступен в *Scans → Tasks*. Такие задачи помечаются отдельной иконкой статуса.

Доступные действия:

- Импортировать отчёты в задачу.
- Переместить задачу в корзину.
- Редактировать, клонировать, экспортировать в XML.

Для пакетных операций используйте кнопки под списком (массовое удаление/экспорт с выбором из выпадающего списка).

Страница детализации импорт-задачи (клик по имени или по значку «Details») содержит вкладки:

- *Information* — общая информация.
- *User Tags* — пользовательские теги (см. разд. 5.1 «Теги»).
- *Permissions* — права доступа (см. гл. 6 «Права и роли»).

В левом верхнем углу доступны действия: открыть справку, перейти к списку, создать новую обычную или импорт-задачу,
клонировать/редактировать/удалить/экспортировать, импортировать отчёты,
открыть последний или все отчёты, просмотреть результаты/заметки/override.

5.6 Управление целями (Targets)

Список целей открывается в *Configuration Targets*. Для каждой цели отображаются: имя, перечень/диапазон хостов, число IP, используемый список портов и привязанные учётные данные.

Действия: удалить (если не используется), редактировать, клонировать, экспортировать XML. Массовые операции доступны под списком.

Детализация цели содержит вкладки *Information*, *User Tags*, *Permissions* и набор действий (справка, к списку, создать новую цель, клон/редактирование/удаление, экспорт).

5.7 Списки портов (Port Lists)

Если сервисы работают на нестандартных портах и их нужно мониторить, используйте пользовательские списки портов. Стандартные списки от Greenbone приходят через ленту SecInfo и обновляются вместе с ней.

Стандартные списки нельзя редактировать. Их может временно удалить только Feed Import Owner или супер-администратор; при следующем обновлении фида они снова будут загружены.

Для постоянного удаления стандартного списка его должен удалить Feed Import Owner, после чего сменить владельца импорта фида на *(Unset)* (см. гл. 4 «Администрирование фида»).

5.7.1 Создание списка портов

1. Откройте *Configuration → Port Lists*.
2. Нажмите **New Port List**.
3. Заполните форму (см. рис. 5.25) и нажмите **Save**.

Рис. 5.25 — Создание списка портов

Поля:

- *Name* — произвольное имя.
- *Comment* — необязательный комментарий.
- *Port Ranges* — диапазоны портов вручную или импортом файла (ASCII). Значения разделяются запятыми. Допустимы одиночные порты (`7`) и диапазоны (`9-11`), с префиксом протокола `T:` (TCP) или `U:` (UDP), например `T:1-3, U:7, 9-11`. Без префикса подразумевается TCP.

5.7.2 Импорт списка портов

1. *Configuration → Port Lists* → **Import**.
2. Выберите XML-файл списка портов → **Import**.

5.7.3 Управление списками портов

На странице *Port Lists* отображаются имя и суммарные счётчики: всего портов, TCP и UDP.

Действия: удалить (если не используется; и пока запись в корзине — она не будет перезагружена фидом), редактировать (только собственные и неиспользуемые), клонировать, экспортировать XML. Массовые операции доступны под списком.

Детализация списка портов показывает *Information*, вкладку *Port Ranges* (первый/последний порт и протокол), *User Tags*, *Permissions* и стандартные действия.

5.8 Управление задачами (Tasks)

Все задачи отображаются на странице *Scans → Tasks* (см. рис. 5.26).

Рис. 5.26 — Страница *Tasks*

Колонки:

- *Name* — имя задачи и индикаторы:
  - Задача изменяемая (alterable) — разрешено менять цель/сканер/конфиг даже после появления отчётов.
  - Запуск на удалённом сканере (см. гл. 8 «Сенсоры и удалённые сканеры»).
  - Задача видима другим пользователям / задача принадлежит другому пользователю.
- *Status* — текущий статус: нет запусков, подготовка, очередь ожидания, выполнение (процент — по числу VT, не по времени), пост-обработка, выполнено, запрос на остановку, остановлено, удалено, ошибка, импорт-задача.
- *Reports* — число отчётов (клик применит фильтр и откроет список соответствующих отчётов).
- *Last Report* — дата/время последнего отчёта (клик — детализация отчёта).
- *Severity* — максимальная найденная опасность по CVSS: Critical (9.0–10.0), High (7.0–8.9), Medium (4.0–6.9), Low (0.1–3.9), Log (0.0).
- *Trend* — динамика уязвимостей между последним и предпоследним отчётом (см. разд. 5.10).

Действия над задачей: запустить (если не выполняется), остановить (результаты будут записаны), показать детали расписания (для плановых задач), возобновить остановленную (незавершённые хосты будут просканированы заново), удалить в корзину, редактировать, клонировать, экспортировать XML. Массовые операции доступны под списком.

Страница детализации задачи содержит вкладки *Information*, *User Tags*, *Permissions* и действия: открыть справку, перейти к списку, создать новую обычную/импорт-задачу, клон/редактирование/удаление/экспорт, запуск/остановка/возобновление, переход к отчётам/результатам/заметкам/override.

5.8.1 Назначение прав доступа к задаче

По умолчанию обычные пользователи не могут создавать права для других пользователей, так как не имеют доступа к базе пользователей. Чтобы выдавать права другим, требуется глобальное и адресное разрешение `get_users` (см. гл. 6.4.3).

1. Откройте *Scans → Tasks*.
2. Кликните по имени задачи и нажмите **Details**, чтобы открыть страницу детализации.
3. Перейдите на вкладку **Permissions**.
4. В секции *Permissions* нажмите **New**.
5. Выберите тип разрешения в списке *Grant*, затем вариант *User*, *Group* или *Role* и укажите конкретного получателя (см. рис. 5.27).
6. Нажмите **Save**.

Рис. 5.27 — Создание нового разрешения

После сохранения разрешение отобразится на странице задачи (см. рис. 5.28). Пользователь увидит задачу и получит доступ к соответствующим отчётам согласно выданным правам.

Рис. 5.28 — Разрешение на странице детализации задачи

5.9 Конфигурации сканирования (Scan Configs)

Конфигурация сканирования определяет набор VT (Network Vulnerability Tests), а также общие и экспертные параметры для движка и отдельных тестов. В поставке НАЙС.ОС Greenbone COMMUNITY EDITION доступны преднастроенные конфигурации; их можно клонировать и на их базе создавать собственные.

5.9.1 Стандартные конфигурации

Базовые профили поставляются через фид и обновляются вместе с ним. Если стандартные профили отсутствуют — обновите фид или назначьте владельца импорта фида (см. гл. 4.10.1).

Стандартные профили редактировать нельзя. Их можно временно удалить (Feed Import Owner или супер-админ); при следующем обновлении фида они появятся снова. Для постоянного удаления профиль должен удалить Feed Import Owner, после чего сменить владельца импорта на *(Unset)*.

Доступные по умолчанию:

- **Empty** — пустой шаблон без VT (статические семьи).
- **Base** — сбор инвентарной информации, без уязвимостей; порт-сканер *Ping Host*; статические семьи.
- **Discovery** — полная инвентаризация (порты, железо, сервисы, ПО, сертификаты); динамические семьи.
- **Host Discovery** — только обнаружение хостов; статические семьи.
- **System Discovery** — обнаружение ОС и оборудования; статические семьи.
- **Full and fast** — оптимальный стартовый профиль: почти все безопасные VT, низкая FN; динамические семьи.
- **Full and fast ultimate** — как выше, плюс потенциально нарушающие работу VT; динамические семьи; возможно больше FP, может потребовать ручной разбор и overrides.
- **Full and very deep** — игнорирует результаты порт-скана при выборе VT, очень медленно; динамические семьи.
- **Full and very deep ultimate** — «very deep» + опасные VT; очень медленно; потенциально больше FP.

5.9.2 Создание собственной конфигурации

Пользовательские профили с `safe_checks = no` могут давать больше ложных срабатываний в зависимости от среды. Для спорных случаев может потребоваться ручной анализ и настройка overrides.

1. Откройте *Configuration → Scan Configs*.
2. Нажмите **New** (или используйте импорт, см. гл. 5.9.3).
3. Задайте *Name* и выберите базу: *Base*, *Empty, static and fast*, *Full and fast* или ранее созданный профиль (см. рис. 5.29).

4. Нажмите **Save** — профиль появится в списке.

Рис. 5.29 — Создание новой конфигурации

5. Для правки общих настроек (семья *Settings*) нажмите **Edit** в строке профиля.
6. Для детальной правки нажмите **All VT Families / Scanner Prefs / VT Prefs** (см. рис. 5.30).

Рис. 5.30 — Редактирование профиля (семьи *VT, prefs)*

- В блоке *Edit Network Vulnerability Test Families* включите авто-активацию новых семей, если нужно, и при необходимости отметьте *Select all NVTs* для выбранных семей.
- Нажмите **Edit** у конкретной семьи для выбора отдельных VT (см. рис. 5.31).

Рис. 5.31 — Выбор *VT* внутри семьи

Семьи LSC для конкретных платформ (например, *Windows Local Security Checks*, *Ubuntu Local Security Checks* и т. п.) недоступны для ручного редактирования.

Для пакетных LSC по SSH обязательно активируйте VT *Determine OS and list of installed packages via SSH login* (OID: `1.3.6.1.4.1.25623.1.0.50282`).

- Нажмите **Edit** у конкретного VT, чтобы настроить его предпочтения (см. рис. 5.32), затем **Save**.
- При необходимости настройте *Scanner Preferences* (см. гл. 5.9.4) и *VT Preferences* (см. гл. 5.9.5).
- Сохраните профиль кнопкой **Save**.

Рис. 5.32 — Настройка параметров конкретного *VT*

5.9.3 Импорт конфигурации сканирования

Импортируйте профили, созданные той же версией GOS, что используется сейчас. Профили из других версий могут вызвать ошибки или некорректное поведение. Профили с предпочтением сканера `safe_checks = no` могут давать повышенное количество ложных срабатываний в зависимости от среды. Для спорных случаев может потребоваться ручной разбор и настройка overrides (см. гл. 6.8).

1. Откройте *Configuration → Scan Configs*.
2. Нажмите **Import**.
3. Нажмите **Browse…** и выберите XML-файл конфигурации.
4. Нажмите **Import**.

Если имя импортируемого профиля уже существует, к имени будет добавлен числовой суффикс.

После импорта профиль появится на странице *Scan Configs*. Для его настройки выполните шаги 6–16 из раздела 5.9.2.

5.9.4 Редактирование предпочтений сканера (Scanner Preferences)

1. Откройте *Configuration → Scan Configs*.
2. В строке нужного профиля нажмите **Edit**.
3. В секции *Edit Scanner Preferences* нажмите **Edit** (см. рис. 5.33).

Рис. 5.33 — Редактирование предпочтений сканера

После внесения изменений нажмите **Save** для сохранения профиля.

5.9.4.1 Описание ключевых предпочтений сканера

Полная документация всех предпочтений выходит за рамки данного руководства. Ниже приведены наиболее важные параметры. Недокументированные опции могут быть помечены как устаревшие и игнорироваться движком.

- **alive_test_ports** — TCP-порты для Boreas при методах *TCP-ACK Service Ping*/*TCP-SYN Service Ping*. Неверные значения заменяются на значения по умолчанию.
- **auto_enable_dependencies** — автоматическое включение VT, от которых зависят другие VT.
- **cgi_path** — путь, используемый VT для доступа к CGI-скриптам.
- **checks_read_timeout** — таймаут сетевых сокетов при сканировании.
- **test_alive_wait_timeout** — ожидание ответов Boreas после отправки последнего пакета (1–20).
- **test_empty_vhost** — дополнительно сканировать с пустым vhost.
- **max_sysload** — порог загрузки аплайнса; при превышении запуск новых VT приостанавливается.
- **min_free_mem** — минимальный свободный объём RAM (МБ); при недостатке запуск новых VT приостанавливается.
- **non_simult_ports** — порты, которые VT не проверяют одновременно.
- **optimize_test** — запускать VT только при выполнении предпосылок (открытый порт, обнаруженное приложение и т. д.).
- **plugins_timeout** — максимальное время работы отдельного VT.
- **safe_checks** — отключить VT, потенциально наносящие ущерб хосту.
- **scanner_plugins_timeout** — лимит (сек.) для семейства *Port scanners*; превышающие VT принудительно завершаются.
- **expand_vhosts** — расширять список vhost данными из rDNS и сертификатов.
- **time_between_request** — пауза (мс) между действиями (открытие сокета/запрос/закрытие).
- **timeout_retry** — число повторов при таймауте соединения.
- **unscanned_closed** — считать не просканированные TCP-порты закрытыми.
- **unscanned_closed_udp** — считать не просканированные UDP-порты закрытыми.

5.9.5 Редактирование предпочтений VT (VT Preferences)

1. Откройте *Configuration Scan Configs*.
2. В строке профиля нажмите **Edit**.
3. В секции *Network Vulnerability Test Preferences* нажмите **Edit**.
4. В строке нужного параметра VT нажмите **Edit**, измените значение и нажмите **Save**.
5. Нажмите **Save** для сохранения профиля.

5.9.5.1 Описание предпочтений VT

Ниже приведены параметры для порт-сканеров *Ping Host* и *Nmap (NASL wrapper)*. Полный перечень опций других VT не рассматривается.

5.9.5.1.1 VT *Ping Host*

- **Report about reachable Hosts** — включить вывод обнаруженных как доступные хостов.

5.9.5.1.2 VT *Nmap (NASL wrapper)*

Опции ниже транслируются в параметры командной строки Nmap (см. документацию Nmap):

- Do not randomize the order in which ports are scanned
- Do not scan targets not in the file (см. *File containing grepable results*)
- Fragment IP packets
- Identify the remote OS
- RPC port scan
- Run dangerous ports even if safe checks are set
- Service scan
- Use hidden option to identify the remote OS
- Data length
- Host Timeout
- Initial RTT timeout
- Max RTT timeout
- Min RTT timeout
- Max Retries
- Maximum wait between probes
- Minimum wait between probes
- Ports scanned in parallel (max/min)
- Source port
- File containing grepable results
- TCP scanning technique
- Timing policy

Профили Timing policy:

Policy	initial_rtt_timeout	min_rtt_timeout	max_rtt_timeout	max_parallelism	scan_delay	max_scan_delay
Paranoid	5 min	100 ms	10 s	serial	5 min	1 s

Policy	initial_rtt_timeout	min_rtt_timeout	max_rtt_timeout	max_parallelism	scan_delay	max_scan_delay
Sneaky	15 s	100 ms	10 s	serial	15 s	1 s
Polite	1 s	100 ms	10 s	serial	400 ms	1 s
Normal	1 s	100 ms	10 s	parallel	0 s	1 s
Aggressive	500 ms	100 ms	1250 ms	parallel	0 s	10 ms
Insane	250 ms	50 ms	300 ms	parallel	0 s	5 ms

5.9.6 Управление конфигурациями сканирования

Страница списка

Все существующие конфигурации сканирования отображаются в меню `Configuration  Scan Configs` (см. рис. 5.34).

Для каждой конфигурации выводится:

- **Name** — имя конфигурации сканирования.
- **Type** — тип конфигурации сканирования.
- **Family – Total** — количество активированных семейств VT.
- **Family – Trend** — тенденция по семействам VT:
  - Новые семейства VT автоматически включаются и активируются после обновления фида.
  - Новые семейства VT не включаются автоматически после обновления фида.
- **NVTs – Total** — количество активированных VT.
- **NVTs – Trend** — тенденция по VT:
  - Новые VT из активированных семейств автоматически включаются и активируются после обновления фида.
  - Новые VT не включаются автоматически после обновления фида.

Примечание. Greenbone регулярно публикует новые VT. Новые семейства VT также могут появляться через OPENVAS ENTERPRISE FEED.

Рис. 5.34 — Страница Scan Configs со всеми доступными конфигурациями

Доступные действия для каждой конфигурации:

- Редактировать общие настройки (семейство **Settings**) — только для собственных

и неиспользуемых.
- Переместить конфигурацию в корзину — только для неиспользуемых собственных; пока объект в корзине, он не будет загружен вновь при следующем обновлении фида.
- Полное редактирование конфигурации — только для неиспользуемых собственных.
- Клонировать конфигурацию.
- Экспортировать конфигурацию в XML.

Примечание. С помощью управляющих элементов под таблицей (массовые операции) можно перемещать в корзину или экспортировать несколько конфигураций.

Страница деталей

Щёлкните по имени конфигурации или нажмите соответствующую кнопку для открытия её страницы.

Доступные вкладки:

- **Scanner Preferences** — все предпочтения сканера (см. разд. 5.9.4.1).
- **NVT Families** — семейства VT, число активированных VT и тренд.
- **NVT Preferences** — предпочтения VT (см. разд. 5.9.5.1).
- **User Tags** — назначенные теги (см. гл. 7.4).
- **Permissions** — назначенные права (см. гл. 8.4).

Действия:

- Открыть соответствующую главу руководства.
- Перейти к списку всех конфигураций.
- Создать новую конфигурацию (см. 5.9.2).
- Клонировать конфигурацию.
- Редактировать (только собственные и неиспользуемые).
- Переместить в корзину (только собственные и неиспользуемые); пока объект в корзине, он не будет загружен вновь при следующем обновлении фида.
- Экспортировать в XML.
- Импортировать конфигурацию (см. 5.9.3).

5.10 Выполнение сканирования по расписанию

Для непрерывного управления уязвимостями предусмотрено планирование задач. Задачи могут выполняться однократно или периодически. По умолчанию расписания отсутствуют.

5.10.1 Создание расписания

1. Откройте `Configuration  Schedules`.
2. Нажмите соответствующую кнопку создания.
3. Задайте параметры (см. рис. 5.35).
4. Нажмите **Save**. Расписание станет доступно при создании задачи (см. 5.2.2).

Рис. 5.35 — Создание расписания

Параметры:

- **Name** — произвольное имя.
- **Comment** — необязательный комментарий.
- **Timezone** — часовой пояс (по умолчанию UTC±00:00).

Примечание. Аплайнс работает во внутреннем поясе UTC±00:00. Для EST выбирайте `America/New_York`.

- **First Run** — дата/время первого запуска (календарь по пиктограмме; *Now* — текущее время).
- **Run Until** — дата/время окончания. Задачи с установленным временем окончания вручную не запускаются. Флажок *Open End* — без конца.
- **Duration** — максимальная длительность окна. По истечении окно закрывается, задача приостанавливается до следующего окна.
- **Recurrence** — периодичность: *Once / Hourly / Daily / Weekly / Monthly / Yearly / Workweeks (Mon–Fri)* либо *Custom*.

5.10.2 Управление расписаниями

Страница списка

Все расписания отображаются в `Configuration  Schedules`.

- **Name** — имя.

- **First Run** — первый запуск.
- **Next Run** — ближайший запуск.
- **Recurrence** — периодичность.
- **Duration** — максимальная длительность окна выполнения.

Действия:

- Переместить в корзину (только неиспользуемые).
- Редактировать.
- Клонировать.
- Экспортировать в XML.

Примечание. Массовые операции доступны под таблицей.

Страница деталей

Откройте расписание по имени или кнопкой перехода.

- **Вкладки:** *Information*, *User Tags* (см. 7.4), *Permissions* (см. 8.4).
- **Действия:** открыть главу; вернуться к списку; создать (5.10.1); клонировать; редактировать; переместить в корзину (неиспользуемые); экспортировать.

5.11 Создание и управление сканерами

Аплайнс содержит два предопределённых сканера. Допускается управление и создание новых.

Доступные сканеры:

- **OpenVAS Default**
- **CVE** — прогноз рисков по текущей SecInfo без повторного сетевого сканирования (см. 5.4 и 13).

Примечание. Сквазер выбирается при создании задачи (см. 5.2.2).

5.11.1 Создание сканера

Примечание. Создание нового сканера используется для добавления удалённого сканера (см. 15.4).

5.11.2 Управление сканерами

Страница списка

Все сканеры отображаются в `Configuration  Scanners` (см. рис. 5.36).

Доступные действия:

- Переместить сканер в корзину (только собственные).
- Редактировать сканер (только собственные).
- Клонировать сканер (только собственные).
- Экспортировать сканер в XML.
- Проверить доступность (*Verify*) — сканер онлайн и доступен менеджеру по сертификатам/учётным данным.

Примечание. Массовые операции доступны под таблицей.

Рис. 5.36 — Страница Scanners

Страница деталей

Откройте страницу сканера по имени или кнопкой перехода.

- **Вкладки:** *Information*, *User Tags* (см. 7.4), *Permissions* (см. 8.4).
- **Действия:** открыть главу; вернуться к списку; создать (5.11.1); клонировать (только собственные); редактировать (только собственные); переместить в корзину (только собственные); экспортировать; *Verify*.

5.12 Использование оповещений (Alerts)

Оповещения встроены в систему. При наступлении заданного события (например, завершение задачи) проверяется условие (например, обнаружена уязвимость высокой категории). Если условие выполняется, выполняется действие — например, отправка письма на заданный адрес.

5.12.1 Создание оповещения

1. Откройте `Configuration  Alerts`.
2. Нажмите кнопку создания.
3. Задайте параметры (см. рис. 5.37).

4. Нажмите **Save**.

Рис. 5.37 — Создание нового оповещения

Параметры оповещения:

- **Name** — произвольное имя.
- **Comment** — необязательный комментарий.
- **Event** — событие, при котором отправляется оповещение. Возможные варианты: смена статуса задачи; добавление/обновление объектов SecInfo (VTs, CVEs, CPEs, CERT-Bund, DFN-CERT); назначение/редактирование тикета (см. 10.6).
- **Condition** — дополнительные условия срабатывания.
  Варианты зависят от типа оповещения: связанное с задачей, SecInfo или тикетом.
  - Всегда (*Always*).
  - При достижении заданного уровня опасности (severity).
  - При изменении/росте/снижении уровня опасности.
  - Если Powerfilter дал не менее указанного числа совпадений больше, чем в предыдущем скане.
- **Report Content** (только для оповещений по задачам) — ограничение содержимого отчёта фильтром. Кнопка открытия компоновщика (*scan report content composer*) позволяет выбрать ранее созданный Powerfilter (см. 10.2.2, 7.3). Опции:
  - *Include*: отметить *Notes* для включения заметок; *Overrides* — пометки и текст переопределений.
  - *Pagination*: *Ignore* — игнорировать пагинацию интерфейса в формируемом отчёте.
- **Details URL** (только для SecInfo) — URL получения SecInfo.
- **Delta Report** (только для задач) — формирование дельта-отчёта относительно предыдущего отчёта или отчёта с указанным ID.
- **Method** — метод доставки. Выбирается один метод на оповещение. Для разных методов на одно событие создаются несколько оповещений.
  Некоторые методы недоступны для оповещений по SecInfo или тикетам.

  Email

  Отправка отчёта на адрес e-mail. Требуется настроенный *mailhub* в админ-меню GOS (см. 6.2.11). Обязательные поля: **To Address**, **From Address**, **Content**. Тема и шифрование — опционально.

- **To Address** — получатель.
- **From Address** — отправитель.
- **Subject** — поддерживаемые плейсхолдеры: `$d`, `$e`, `$n`, `$N`, `$q`, `$s`, `$S`, `$T`, `$u`, `$U`, `$$`.
- **Email Encryption** — шифрование S/MIME или PGP.
  - S/MIME: PEM, X.509; выдан на адрес получателя; валиден; полный chain; без приватного ключа.
- **Content**:
  - *Include Report* — включить отчёт в тело письма (только текстовые форматы `text/*`). Для *Customizable CSV Results* выбрать *Report Config*.
  - *Attach Report* — приложить отчёт (любой формат; для настраиваемых — выбрать *Report Config*).
  - Плейсхолдеры в сообщении: `$c`, `$d`, `$e`, `$F`, `$f`, `$H`, `$i`, `$n`, `$N`, `$q`, `$r`, `$s`, `$S`, `$t`, `$T`, `$u`, `$U`, `$z`, `$$`.

HTTP Get

Вызов URL по HTTP GET (например, шлюз SMS или создание задачи в баг-трекере). Плейсхолдеры: `$n`, `$e`, `$c`, `$$`. Пример: `https://example.com/$n` → `.../Scan_task_1`.

SCP

Копирование отчёта по SCP.

- **Credential** — (user+password) или (user+SSH key).
- **Host** — имя/адрес назначения; **Port** — 1–65535 (по умолчанию 22).
- **Known Hosts** — публичный ключ SSH сервера в формате `host algo public_key`; *host* должен совпадать с **Host**.
- **Path** — полный путь к файлу, напр. `/home/user/report.xml`. В имени файла доступны `$$`, `$n`.
- **Report** — формат; при настраиваемых — **Report Config**.

Send to host

Отправка отчёта на произвольный *host:port* по TCP. Поддерживаются установленные форматы отчётов; при настраиваемых — *Report Config*.

SMB

Копирование отчёта по SMB.

- **Credential** — учётные данные (user+password).

- **Share path** — UNC вида `\\host\share` (должна существовать).
- **File path** — путь внутри шара; при отсутствии подпапок — создаются. Расширение добавляется по формату отчёта. Если путь оканчивается `\`, добавляется имя по умолчанию (см. 7.7).
- Тег задачи `smb-alert:file_path` переопределяет путь (см. 7.4).
- Плейсхолдеры: `%C`, `%c`, `%D`, `%F`, `%M`, `%m`, `%N`, `%T`, `%t`, `%U`, `%u`, `%%`.
- **Report Format**, **Report Config** — по необходимости.
- **Max Protocol** — *Default* / *SMB3* / *SMB2* / *NT1*.

SNMP

Отправка SNMP trap на заданный агент (с community). Плейсхолдеры: `$$`, `$d`, `$e`, `$n`, `$q`, `$s`, `$S`, `$T`.

Sourcefire Connector

Отправка данных в Cisco Firepower Management Center (см. 17.3).

Start Task

Запуск дополнительной задачи (выбор из списка).

System Logger

Отправка в Syslog (сервер настраивается в 6.2.12). Тайм-стемпы — в поясе UTC±00:00, если иное не задано на syslog-сервере.

verinice.PRO Connector

Отправка данных в verinice.PRO (см. 17.1).

TippingPoint SMS

Загрузка CSV-отчёта по HTTPS API в TippingPoint SMS.

- **Hostname / IP** — адрес (`https://<address>/vulnscanner/import`).
- **Credentials** — учётные данные.
- **SSL / TLS Certificate** — CA-сертификат в PEM/X.505.
- **Use workaround for default certificate** — исправление CN *Tippingpoint*.

Alemba vFire

Создание тикета в vFire с возможностью прикрепления отчётов (см. 17.4).

5.12.2 Назначение существующего оповещения задаче

Редактирование уже используемой задачи допустимо и не влияет на ранее созданные отчёты.

1. Откройте `Scans  Tasks`.
2. В строке задачи нажмите кнопку редактирования.
3. В поле **Alerts** выберите оповещение (см. рис. 5.38). Новый alert можно создать по соответствующей кнопке.
4. Нажмите **Save**.

Рис. 5.38 — Настройка задачи с оповещением

После назначения задача появится на странице деталей оповещения (см. рис. 5.39).

Рис. 5.39 — Задача, использующая конкретное оповещение

5.12.3 Управление оповещениями

Страница списка

Все оповещения — в `Configuration  Alerts`.

Отображаются поля:

- **Name** — имя.
- **Event** — событие.
- **Condition** — условие срабатывания.
- **Method** — метод (с деталями назначения, например IP/e-mail).
- **Filter** (для задач) — фильтр отчёта.
- **Active** — признак включения/выключения.

Действия:

- Переместить в корзину (только неиспользуемые).
- Редактировать.
- Клонировать.
- Экспортировать в XML.

- Тестировать оповещение.

Массовые операции перемещения/экспорта доступны под таблицей.

Страница деталей

Откройте по имени или кнопкой перехода.

- **Вкладки:** *Information*, *User Tags* (см. 7.4), *Permissions* (см. 8.4).
- **Действия:** открыть главу; перейти к списку; создать (см. 5.12.1); клонировать; редактировать; переместить в корзину (неиспользуемые); экспортировать в XML.

5.13 Типовые препятствия при сканировании

Несмотря на корректные значения по умолчанию для большинства сред, реальные условия и настройки цели могут требовать тонкой настройки.

5.13.1 Хосты не обнаружены

По умолчанию (Discovery или Full and fast) предварительно выполняется *ping* цели. Если отклика нет, хост считается недоступным и не сканируется порт-сканером/VT.

Причина — фильтрация ICMP локальными фаерволами и т.п. Решение — настроить **Alive Test** в цели и/или конфигурации сканирования:

- TCP-ping (ACK/SYN) при отсутствии ICMP-ответа.
- ARP-ping в одной широковещательной доменной (L2).

5.13.2 Длительные сканы

После подтверждения «живости» выполняется порт-скан. По умолчанию используется TCP-список 5000 портов. Если фаервол дропает пакеты, сканер ждёт таймаут для каждого порта (особенно критично при включении UDP). Рекомендации:

- Тюнить порт-листы под фактически используемые порты.
- Настроить фаерволы на *reject* вместо *drop* (где допустимо) для ускорения таймаутов.

5.13.3 VT не выполняется

Часто касается UDP-VT (например, SNMP). В *Full and fast* SNMP-VT включены, но при стандартном TCP-только порт-листе 161/UDP не обнаруживается — соответствующие VT не запускаются.

Не включайте «все порты» по умолчанию — это значительно увеличит длительность. Лучший подход — точечно расширять порт-листы под нужные сервисы и правила фаерволов.

5.13.4 Сканирование vhosts

Сканер автоматически выявляет связи имён и IP без дополнительного ввода. В средах с виртуальными хостами отчёты содержат меньше дубликатов.

Параметры сканера (см. 5.9.4), влияющие на vhosts:

- `test_empty_vhost` — дополнительно тестировать с пустыми vhost-значениями.
- `expand_vhosts` — расширять список vhost на основе reverse-lookup и данных из сертификатов SSL/TLS и VT.